



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,308	08/26/2003	Shigenori Miyauchi	67161-089	2605
<div>7590      07/03/2007</div> <div>McDermott, Will &amp; Emery 600 13th Street, N.W. Washington, DC 20005-3096</div>				
			EXAMINER PAN, JOSEPH T	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 07/03/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/647,308

Applicant(s)

MIYAUCHI ET AL.

Examiner

Joseph Pan

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 8/26/03.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. The applicant's response filed on April 2, 2007 has been fully considered. Claim 1 has been amended. Claims 1-7 are pending.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monier (U.S. Patent No. 5,987,489) in view of Shimbo (U.S. Patent No. 6,088,453).

#### Referring to claim 1:

i. Monier teaches:

An encryption circuit, comprising:

a plurality of operation circuits which are connected (see e.g. figure 3 of Monier); and

a control circuit controlling said plurality of operation circuits to provide encryption or decryption control (see column 6, lines 23-28 of Monier); wherein each of said plurality of operation circuits includes

a first register holding operation data (see e.g. figure 3, element 11 of Monier),

an addition and subtraction circuit performing addition and subtraction with respect to the operation data held in said first register (see figure 3, element 28 of Monier),

a right-shift circuit performing right-shift with respect to an operation result by said addition and subtraction circuit (see column 6, lines 37-39 of Monier), and

a second register holding an operation result by said right-shift circuit (see column 7, lines 30-39 of Monier);

an addition and subtraction circuit in a first operation circuit performs addition and subtraction using a carry-in signal from a second operation circuit, and outputs a carry-out signal generated through addition and subtraction to a third operation circuit (see figure 3, element 28; and column 7, lines 30-39 of Monier); and

a right-shift circuit in said first operation circuit performs right-shift using a shift-in signal from said third operation circuit, and outputs a shift-out signal generated through right-shift to said second operation circuit (see column 6, lines 37-39 of Monier).

Monier discloses the addition circuit and the subtraction circuit. However, Monier does not specifically mention the addition and subtraction circuit.

Also, Monier discloses the shift registers (see column 3, lines 46-49). However, Monier does not specifically mention that one right-shift circuit uses a right-shift in signal from another right shift circuit.

ii. Shimbo teaches a scheme for performing high speed Montgomery division wherein Shimbo discloses the Adder/Subtractor (see figure 14, element 806 'adder/subtractor'; and column 22, line 28 of Shimbo). Shimbo further discloses that one shift circuit uses a right-shift in signal from another shift circuit (see figure 7C; and column 11, lines 40-43 of Shimbo).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shimbo into the method of Monier to use the addition and subtraction circuit for the encryption unit.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shimbo into the method of Monier to make one right-shift circuit uses a right-shift in signal from another right shift circuit.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Shimbo into the system of Monier to use the addition and subtraction circuit for the encryption unit, because the addition and the subtraction circuit supports the functionalities of both the addition circuit or the subtraction circuit.

The ordinary skilled person would have been motivated to have applied the teaching of Shimbo into the system of Monier to make one right-shift circuit uses a right-shift in signal from another right shift circuit, because Shimbo discloses "This procedure utilizes four multiple-precision registers referred to as registers U, V, T and S, and is constructed from left and right shifting operations on registers and additions and subtractions among registers." (see column 11, lines 38-41 of Shimbo), and Monier also utilizes multiple registers (see e.g. figure 3, elements 10, 11, 12). Therefore, Shimbo's teaching could enhance Monier's method.

Referring to claim 2:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the dividing the operand (see column 4, lines 1-8 of Monier).

Referring to claim 3:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the carry value and the clock (see column 12, lines 59-61; and column 11, lines 1-9 of Monier).

Referring to claim 4:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the most significant bit (see column 3, lines 52-53 of Monier).

Referring to claim 5:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the plurality of operation circuits are connected (see figure 3 of Monier).

Referring to claim 6:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the left-shift circuit (see figure 7C; and column 11, lines 40-43 of Shimbo).

Referring to claim 7:

Monier and Shimbo teach the claimed subject matter: an encryption circuit (see claim 1 above). They further disclose the selector (see column 7, lines 44-45 of Monier).

### ***Response to Arguments***

4. Applicant's arguments, filed on April 2, 2007, with respect to that the cited references do not disclose or suggest that one right-shift circuit uses a right-shift in signal from another right shift circuit, have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Shimbo (U.S. Patent No. 6,088,453).

### ***Conclusion***

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

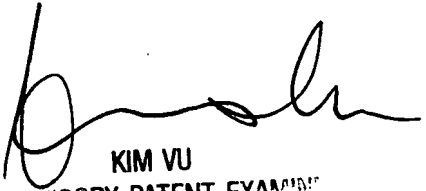
Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan

June 12, 2007



KIM VU  
ASSISTANT PATENT EXAMINER  
TECHNOLOGY CENTER 210